МОУ «Громовская СОШ»

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА К ТВОРЧЕСКОМУ ПРОЕКТУ

D-MASH (DECENTRALIZED MESSENGER WITH ASYMMETRIC-KEY ENCRYPTION AND SECURITY HARDENING)

Разработка прототипа децентрализованного мессенджера с усиленной системой безопасности и резервными каналами связи

Ученик: _____С.С. Генералов

Руководитель: _____Ю.Б. Паршикова

Г. Приозерск

2025

РЕФЕРАТ

Пояснительная записка содержит 24 страницы, 5 рисунков, 2 таблицы, 6 источников, 2 приложения.

Ключевые слова: информационная безопасность, децентрализация, мессенджер, E2EE, правдоподобное отрицание, обход блокировок, P2P, RSA, AES, анализ трафика.

Объект исследования: Методы и протоколы обеспечения конфиденциальности в современных системах обмена сообщениями.

Предмет исследования: Архитектура и протоколы децентрализованного мессенджера, устойчивого к таргетированным атакам, сетевым блокировкам и физической компрометации.

Цель работы: Спроектировать прототип P2P-мессенджера D-MASH, обеспечивающего повышенный уровень приватности за счет децентрализации, системы «Decoy System» и резервного канала связи «PhantomCall».

Методы исследования: Анализ существующих решений, системное проектирование, моделирование угроз, разработка протоколов.

Результаты и новизна: Предложена оригинальная архитектура, не имеющая прямых аналогов, основанная на трех уникальных компонентах. **Во-первых,** система «Decoy System» обеспечивает правдоподобное отрицание при физическом принуждении через систему нескольких паролей. **Во-вторых,** «Tact Protocol» маскирует активность пользователя для защиты от анализа трафика. **В-третьих, «**PhantomCall Protocol» позволяет передавать цифровые данные через голосовые каналы сотовой связи для обхода интернет-блокировок. **Наконец,** «GhostVoice Protocol» обеспечивает проведение конфиденциальных голосовых переговоров в реальном времени путем обратимого искажения (скремблирования) речи.

Область применения: Защищенные коммуникации для пользователей с повышенными требованиями к приватности в условиях цензуры.

СОДЕРЖАНИЕ

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

Сокращение	Расшифровка
D-MASH	Decentralized Messenger with Asymmetric-Key Encryption and Security Hardening
E2EE	End-to-End Encryption (Сквозное шифрование)
PCP	PhantomCall Protocol
P2P	Peer-to-Peer (Пиринговая, одноранговая сеть)
AES	Advanced Encryption Standard (Симметричный алгоритм шифрования)
GCM	Galois/Counter Mode (Режим аутентифицированного шифрования)
MFSK	Multi-frequency shift keying (Многочастотная манипуляция)
NAT	Network Address Translation (Преобразование сетевых адресов)
RSA	Rivest-Shamir-Adleman (Асимметричный алгоритм шифрования)
TURN	Traversal Using Relays around NAT (Обход NAT с использованием ретранслятора)
ИБ	Информационная безопасность
ПО	Программное обеспечение
СОРМ	Система технических средств для обеспечения функций оперативно-разыскных мероприятий

ВВЕДЕНИЕ

В современную цифровую эпоху конфиденциальность личных и профессиональных коммуникаций находится под постоянной угрозой. Глобальная централизация интернет-сервисов, усиление государственного контроля и рост киберпреступности создают среду, в которой популярные мессенджеры перестают быть надежным инструментом для защищенного общения. Существующие решения, несмотря на маркетинговые заявления о безопасности, обладают фундаментальными архитектурными недостатками, которые могут быть и уже используются для компрометации данных пользователей.

Актуальность данного проекта обусловлена наличием доказанных уязвимостей в доминирующих на рынке мессенджерах:

- **Telegram:** Основной режим работы («облачные чаты») **не использует сквозное шифрование по умолчанию.** Это подтверждается простым экспериментом: пользователь, имея активную сессию только на одном устройстве (телефон), может выключить его, авторизоваться на совершенно новом устройстве (ПК) и получить полный доступ ко всей истории переписки. Это однозначно доказывает, что ключи для дешифрования сообщений хранятся на серверах Telegram, что полностью нивелирует концепцию E2EE и дает компании или третьим лицам, получившим доступ к серверам, возможность прочитать всю переписку.
- **WhatsApp**[1]**:** Несмотря на наличие E2EE по умолчанию, система имеет критическую уязвимость в виде **резервных копий.** Долгое время резервные копии чатов, сохраняемые пользователями в облачные хранилища Google Drive или iCloud, не шифровались сквозным ключом. Это создавало бэкдор для доступа к данным. Даже с появлением

1 Принадлежит Meta, признанной в РФ экстремистской организацией, ее деятельность запрещена.

опционального шифрования бэкапов, централизованная архитектура Meta позволяет собирать огромные объемы метаданных (кто, с кем, когда и как долго общался), что является ценной информацией для профилирования и наблюдения.

- **Signal:** Считается наиболее защищенным решением, однако его архитектура по-прежнему **централизована** и требует **привязки к номеру телефона.** Это создает две стратегические проблемы: уязвимость к блокировкам на уровне целых стран путем блокировки IP-адресов серверов Signal, а также проблему деанонимизации пользователя и возможность построения графа его социальных связей.

Таким образом, существует острая и нерешенная проблема отсутствия на рынке массового коммуникационного инструмента, который бы комплексно защищал пользователя от всех векторов атак: от перехвата трафика до физического принуждения.

Цель проекта: спроектировать и описать прототип защищенного P2P-мессенджера D-MASH, обеспечивающего качественно новый уровень приватности и устойчивости к блокировкам.

Для достижения поставленной цели необходимо решить следующие **задачи:**

- провести анализ уязвимостей существующих централизованных мессенджеров;
- разработать полностью децентрализованную сетевую архитектуру на основе P2P;
- спроектировать криптографическое ядро, обеспечивающее надежное E2EE;

- разработать протокол «Decoy System» для обеспечения правдоподобного отрицания;
- разработать комплекс протоколов для экстренной связи через голосовые каналы:
  - «PhantomCall Protocol» для передачи цифровых данных;
  - «GhostVoice Protocol» для проведения защищенных голосовых вызовов.

Объект исследования: Методы и протоколы обеспечения конфиденциальности в современных системах обмена сообщениями.

Предмет исследования: Архитектура и протоколы децентрализованного мессенджера D-MASH.

Пояснительная записка имеет следующую структуру: в первой главе приводится анализ предметной области, во второй главе детально описывается проектируемая архитектура и ключевые протоколы системы D-MASH.

1 АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ И СУЩЕСТВУЮЩИХ РЕШЕНИЙ

1.1 Обзор современных угроз конфиденциальности коммуникаций

Современная модель угроз для пользователей систем обмена мгновенными сообщениями является многоуровневой и затрагивает как сам канал передачи данных, так и конечные устройства. Для разработки комплексной системы защиты необходимо учитывать весь спектр потенциальных векторов атак.

Ключевые угрозы включают:

- **Пассивное прослушивание (Eavesdropping):** Перехват и анализ сетевого трафика на различных участках сети — от локальной Wi-Fi сети до магистральных каналов провайдеров. Без надежного шифрования это позволяет злоумышленнику прочитать содержимое сообщений.
- **Атаки «человек посередине» (Man-in-the-Middle, MITM):** Активная атака, при которой злоумышленник встраивается в канал связи между двумя сторонами, имея возможность не только читать, но и модифицировать передаваемые данные. Для противодействия требуются механизмы аутентификации ключей.
- **Анализ метаданных:** Даже при использовании сквозного шифрования, централизованные серверы собирают и хранят метаданные: идентификаторы отправителя и получателя, время отправки, частоту и продолжительность сеансов связи, IP-адреса. Анализ этих данных позволяет составить подробный социальный граф пользователя и сделать выводы о его деятельности.
- **Сетевые блокировки и цензура:** Государственные регуляторы или интернет-провайдеры могут блокировать доступ к центральным серверам

мессенджера по IP-адресам или доменным именам (технология DPI), делая сервис полностью недоступным в регионе.

- **Компрометация централизованной инфраструктуры:** Серверы мессенджера являются единой точкой отказа. Их взлом или юридическое принуждение владельцев к сотрудничеству может привести к массовой утечке пользовательских данных или ключей шифрования.
- **Физическая компрометация устройства:** Наиболее прямая угроза, при которой злоумышленник получает физический доступ к устройству пользователя (например, в результате изъятия) и принуждает его предоставить пароль или биометрические данные для разблокировки. Стандартные мессенджеры не предоставляют механизмов защиты в таком сценарии.

Комплексная система защиты должна обеспечивать противодействие угрозам на каждом из этих уровней, что не достигается в полной мере ни одним из существующих популярных решений.

1.2 Критический анализ аналогов: Telegram, WhatsApp, Signal

Для оценки текущего состояния рынка был проведен сравнительный анализ трех ключевых игроков по критериям, вытекающим из описанной модели угроз. Результаты анализа сведены в Таблицу 1.1.

Критерий	Telegram	WhatsApp	Signal	D-MASH
Архитектура	Централизованная	Централизованная	Централизованная	Децентрализованная (P2P)
E2EE по умолч.	Нет (только в Secret Chats)	Да	Да	Да
Привязка к номеру	Да	Да	Да	Нет
Сбор метаданных	Высокий	Высокий	Минимальный	Теоретический минимум
Устойчивость к блок.	Низкая	Низкая	Низкая	Высокая (P2P + PCP)
Защита от принужд.	Нет	Нет	Нет	Да

Таблица 1.1 – Сравнительный анализ мессенджеров по ключевым параметрам безопасности

Как следует из проведенного анализа, каждое из популярных приложений имеет одну или несколько фундаментальных уязвимостей. **Telegram** жертвует конфиденциальностью ради удобства, храня ключи на сервере. **WhatsApp**, принадлежащий Meta, является инструментом для массового сбора метаданных. Даже эталонный **Signal** уязвим для блокировок и деанонимизации из-за своей централизованной природы и привязки к номеру телефона.

Ни одно из рассмотренных решений не предлагает механизма защиты от физического принуждения, оставляя пользователя беззащитным в случае изъятия устройства. Этот системный пробел в безопасности современных коммуникационных инструментов и призван решить проектируемый мессенджер D-MASH, архитектура которого будет рассмотрена в следующей главе.

2 ПРОЕКТИРОВАНИЕ АРХИТЕКТУРЫ И ПРОТОКОЛОВ СИСТЕМЫ D-MASH

На основе анализа существующих решений и выявленных уязвимостей была спроектирована архитектура децентрализованного мессенджера D-MASH, нацеленная на комплексное решение проблем безопасности, приватности и устойчивости к блокировкам.

2.1 Общая архитектура и криптографическое ядро

D-MASH строится на гибридной P2P-архитектуре, исключающей центральные серверы для хранения или обработки сообщений. Основной обмен данными происходит напрямую между пользователями (пирами). Для решения проблемы установления соединения между клиентами, находящимися за NAT, а также для первоначального поиска контактов, используется добровольческая сеть вспомогательных Rendezvous/TURN-серверов. Эти серверы выполняют исключительно инфраструктурную роль и не имеют доступа к содержимому передаваемых данных.

- **Идентификация:** Пользователь идентифицируется хешем от своего публичного ключа RSA (UserID), что полностью исключает привязку к личным данным, таким как номер телефона или адрес электронной почты.
- **Криптографическое ядро:** В основе системы лежит стандартная и проверенная гибридная схема сквозного шифрования. Для каждого сообщения генерируется одноразовый сессионный ключ AES-256, которым шифруется содержимое сообщения в режиме GCM (Galois/Counter Mode), обеспечивающем одновременно конфиденциальность и целостность. Сам сессионный ключ асимметрично

шифруется публичным ключом RSA-4096 получателя. Целостность и авторство всего пакета данных подтверждается электронной подписью отправителя, созданной с помощью его приватного ключа RSA.

2.2 Сетевой уровень: «Тактовый протокол» и P2P-маршрутизация

Для защиты от анализа трафика, являющегося одной из ключевых угроз при использовании даже зашифрованных каналов, в D-MASH вводится «Тактовый протокол» (Tact Protocol). Вместо отправки сообщений по мере их написания, клиенты раз в фиксированный интервал времени (1-2 секунды) обмениваются унифицированными пакетами-«тактами». Эти пакеты содержат как новые сообщения, так и транзитный трафик для других участников сети. Такой подход создает постоянный фоновый "шум", значительно усложняя для внешнего наблюдателя определение реальной активности пользователя: является ли он инициатором коммуникации или просто узлом-ретранслятором.

Маршрутизация сообщений между пользователями, не являющимися пирами первого ранга, происходит по цепочке доверенных пиров ("правило 6 рукопожатий"). Поиск маршрута инициируется специальным широковещательным запросом (ROUTE_PROBE). При нахождении получателя маршрут подтверждается обратным сигналом (ROUTE_REPLY), и каждый узел в цепи сохраняет у себя временную запись о маршруте. При этом каждый узел знает только своего соседа слева и справа, но не имеет информации о полном пути следования пакета, что обеспечивает анонимность на сетевом уровне.

2.3 Система правдоподобного отрицания «Decoy System»

Ключевой инновацией проекта, направленной на защиту от физического принуждения, является система «Decoy System». Данная система обеспечивает правдоподобное отрицание (Plausible Deniability) путем создания

многоуровневого доступа к данным, основанного на использовании трех различных паролей.

- **Основной пароль:** Предоставляет стандартный доступ ко всем чатам и функциям приложения.
- **Пароль под принуждением:** Активирует режим "ложного дна". При вводе этого пароля приложение загружает альтернативный, "чистый" профиль, содержащий только заранее определенные безобидные чаты. Настоящие, секретные чаты при этом выгружаются из основной базы данных в отдельный, непробиваемо зашифрованный контейнер, а ключевые контакты могут быть оповещены о тревоге. Для внешнего наблюдателя приложение выглядит полностью функциональным, и он не может доказать наличие скрытых данных.
- **Пароль паники:** Активирует протокол "выжженной земли". При его вводе все данные приложения, включая ключи шифрования и зашифрованные базы данных, немедленно и безвозвратно уничтожаются с устройства с использованием методов безопасного стирания.

Данная система обеспечивает защиту в наиболее критическом сценарии — при физической компрометации устройства и принуждении владельца к сотрудничеству.

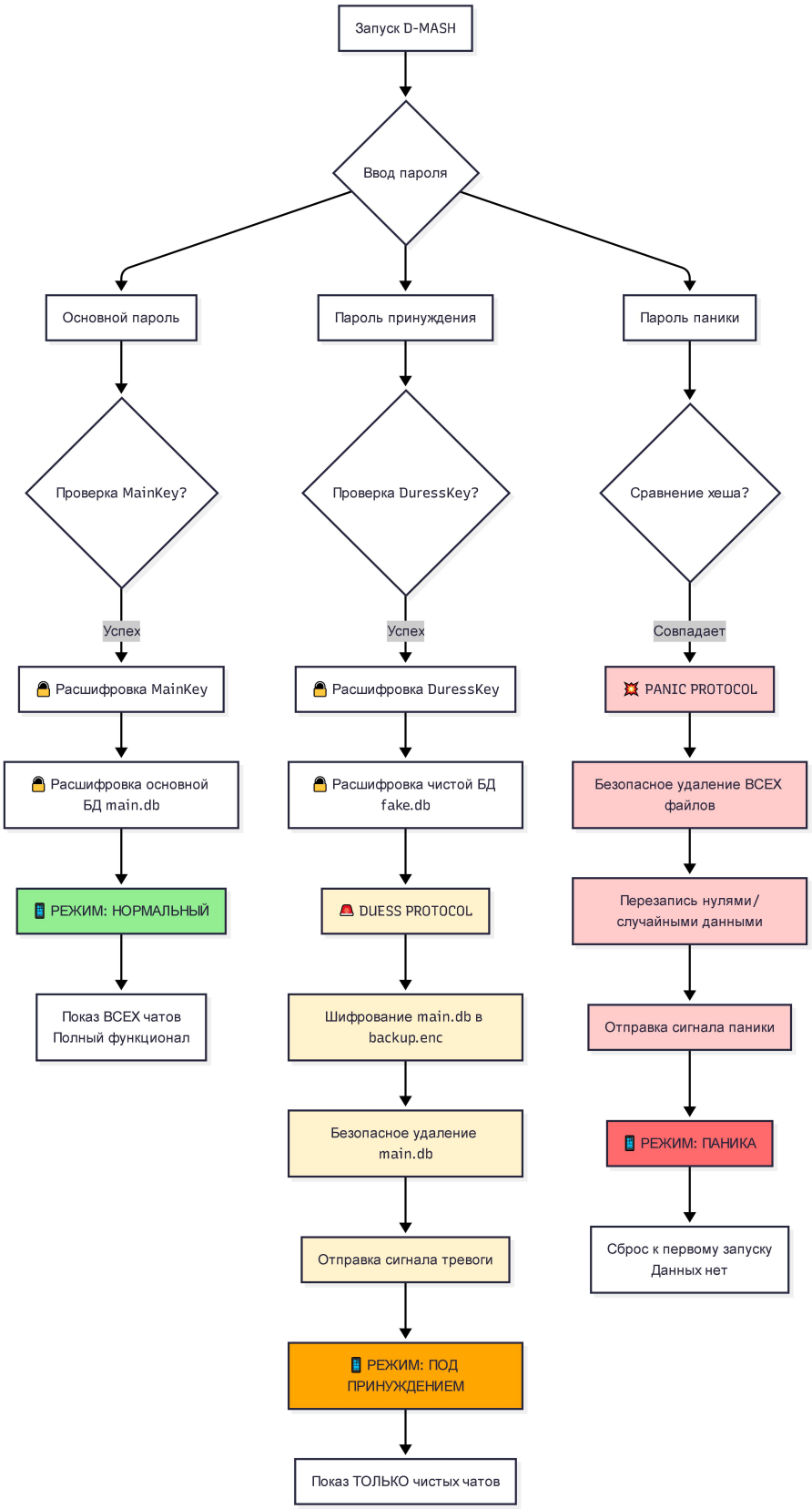

Рисунок 2.1 – Логическая схема работы Decoy System

2.4 Комплекс протоколов экстренной связи через голосовые каналы

Для обеспечения максимальной устойчивости системы к блокировкам и сохранения связи в экстремальных условиях, когда интернет-доступ полностью отсутствует, в D-MASH разработан уникальный комплекс из двух протоколов, использующих для работы **голосовые каналы сотовой связи.** Эти протоколы решают разные задачи — передачу данных и защиту переговоров, — но оба используют один и тот же принцип: маскировку под легитимный голосовой вызов.

2.4.1 PhantomCall Protocol (PCP) для передачи цифровых данных

«PhantomCall Protocol» является резервным транспортным модулем для гарантированной доставки цифровых данных.

- **Принцип работы:** Критически важные данные D-MASH (например, сигнал тревоги из Decoy System, GPS-координаты, текстовое сообщение или ключ шифрования) кодируются в аудиосигнал с помощью устойчивой к помехам модуляции MFSK (Multi-frequency shift keying). Этот аудиосигнал маскируется под фоновый шум и передается в рамках обычного голосового вызова.
- **Скрытность и надежность:** Для систем мониторинга оператора связи (СОРМ) такая передача выглядит как обычный короткий звонок с плохим качеством связи. Протокол невосприимчив к DPI и любым методам блокировки интернет-трафика. Скорость передачи данных низка (порядка 100-200 бит/с), однако этого достаточно для доставки коротких экстренных сообщений.
- **Применение:** Хотя пропускная способность PCP недостаточна для звонков в реальном времени, он идеально подходит для асинхронной передачи небольших пакетов данных, включая сильно сжатые короткие голосовые «SOS-сообщения» (до 5-10 секунд), которые могут быть разбиты на пакеты и переданы в течение нескольких сеансов связи.

2.4.2 GhostVoice Protocol для защищенных голосовых вызовов

В отличие от PCP, протокол «GhostVoice» предназначен не для передачи данных, а для обеспечения конфиденциальности голосовых переговоров в реальном времени.

- **Принцип работы:** Протокол использует не цифровое шифрование, а голосовое скремблирование — применение к аудиосигналу речи обратимых искажений в реальном времени. Перед вызовом стороны по защищенному интернет-каналу обмениваются сессионным ключом скремблирования. В начале вызова специальный звуковой маркер активирует на обеих сторонах режим защиты.
- **Методы скремблирования:** На основе ключа к голосу применяются такие алгоритмы, как инверсия спектра (высокие частоты становятся низкими и наоборот) и частотные скачки (полосы частот постоянно меняются местами). В результате речь становится совершенно неразборчивой для человеческого уха и систем автоматического распознавания, но при этом сохраняет общие характеристики голосового сигнала и без проблем проходит через кодеки оператора. На приемной стороне приложение, зная ключ, применяет те же преобразования в обратном порядке, восстанавливая исходную речь.
- **Применение:** Протокол позволяет вести полноценный, конфиденциальный разговор в реальном времени в условиях, когда доступен только голосовой канал сотовой связи. Это эффективное средство защиты от массовой автоматической прослушки и анализа переговоров.

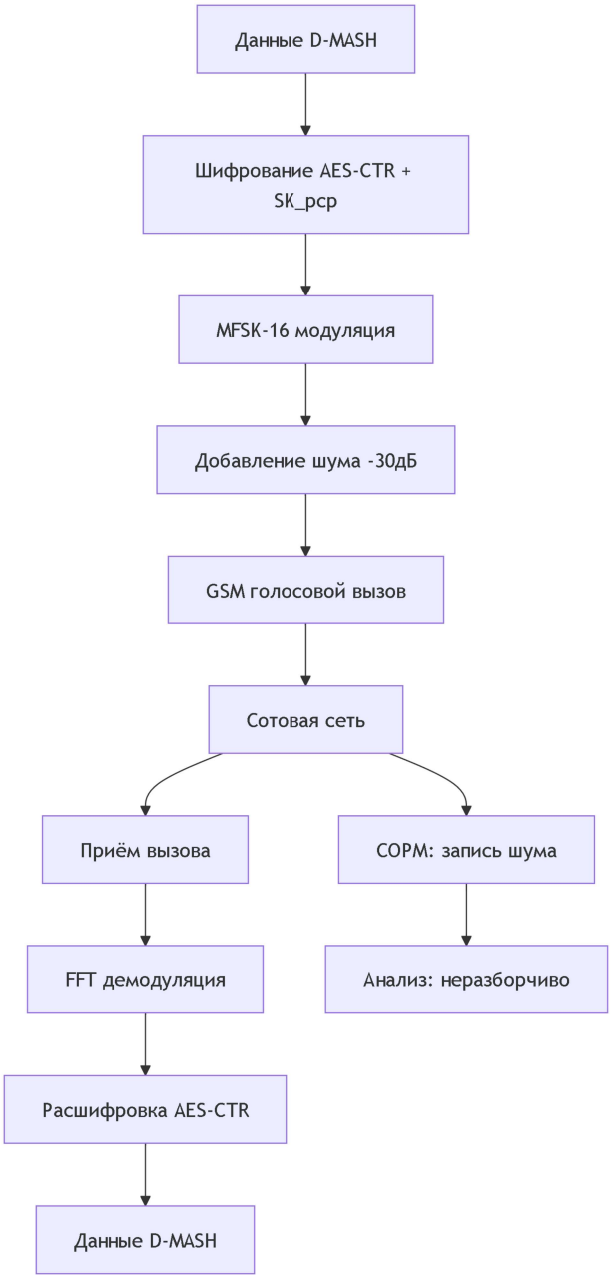

Рисунок 2.2 – Принцип работы PhantomCall Protocol

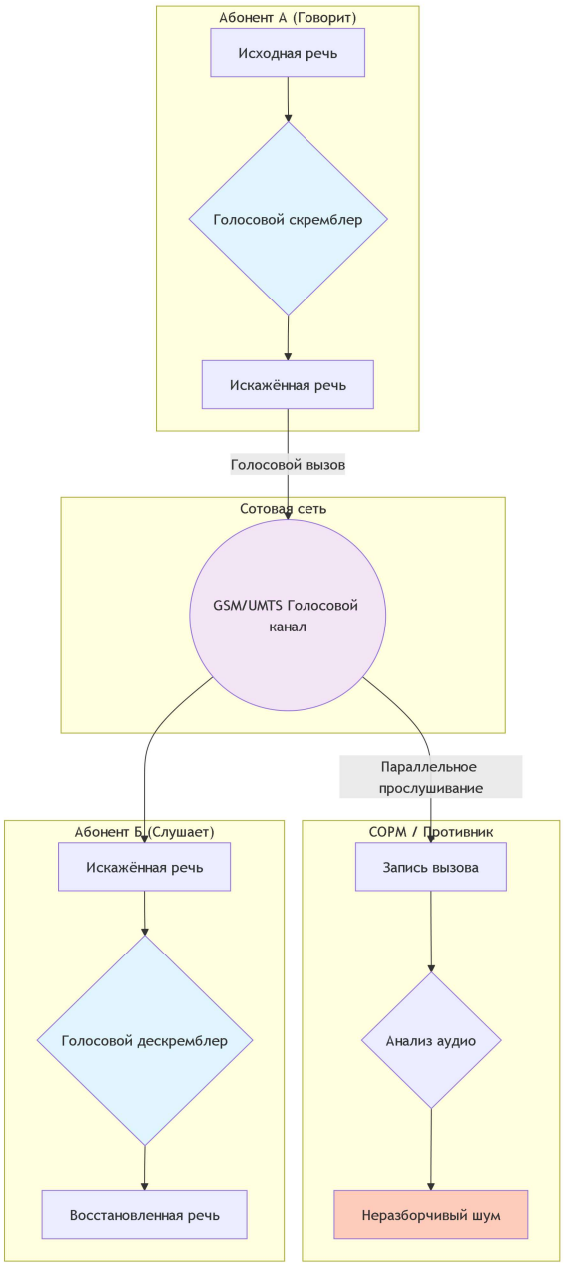

Рисунок 2.3 – Принцип работы GhostVoice Protocol

ЗАКЛЮЧЕНИЕ

В ходе выполнения данного творческого проекта была решена поставленная задача: спроектирована и детально описана архитектура децентрализованного мессенджера D-MASH, обладающего уникальными, комплексно реализованными свойствами безопасности.

В результате проделанной работы были получены следующие ключевые результаты:

- **Проведен анализ,** выявивший фундаментальные уязвимости централизованных архитектур популярных мессенджеров (Telegram, WhatsApp, Signal), включая проблемы с E2EE по умолчанию, сбором метаданных, уязвимостью к блокировкам и отсутствием защиты от физического принуждения.
- **Предложена оригинальная гибридная P2P-архитектура**, устойчивая к блокировкам за счет отсутствия единой точки отказа и обеспечивающая анонимность пользователей путем идентификации по криптографическим ключам и использования многоуровневой маршрутизации.
- **Разработана система «Decoy System»** — инновационный механизм правдоподобного отрицания на основе трех паролей. Данная система обеспечивает защиту в наиболее критическом сценарии — при физической компрометации устройства, — решая проблему, которую игнорируют все существующие аналоги.
- **Разработан комплекс протоколов экстренной связи** через голосовые каналы сотовой сети, включающий «PhantomCall Protocol» для передачи цифровых данных и «GhostVoice Protocol» для проведения конфиденциальных переговоров. Этот комплекс позволяет сохранять связь даже в условиях полного отключения интернета, что является уникальной особенностью проекта.

Таким образом, представленный проект D-MASH, даже на уровне концепции, демонстрирует возможность создания коммуникационной системы, где безопасность, приватность и устойчивость к цензуре являются не опциональными функциями, а базовым, неотъемлемым принципом архитектуры.

Дальнейшее развитие проекта предполагает создание и тестирование рабочего программного прототипа для валидации ключевых протоколов в реальных условиях эксплуатации, а также проведение исследований в области оптимизации производительности P2P-сети и стойкости протоколов скремблирования к современным методам анализа сигналов.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. ГОСТ 7.32-2017. Система стандартов по информации, библиотечному и издательскому делу. Отчет о научно-исследовательской работе. Структура и правила оформления. – Введ. 2018-07-01. – Москва : Стандартинформ, 2017. – 24 с.
2. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер ; пер. с англ. – 2-е изд. – Москва : Триумф, 2003. – 816 с. – ISBN 5-89392-055-4.
3. Таненбаум, Э. Компьютерные сети / Э. Таненбаум, Д. Уэзеролл ; пер. с англ. – 5-е изд. – Санкт-Петербург : Питер, 2012. – 960 с. – ISBN 978-5-459-00342-0.
4. Marlinspike, M., & Perrin, T. The Signal Protocol. – Текст : электронный // Signal. – 2016. – URL: https://signal.org/docs/specifications/doubleratchet/ (дата обращения: 15.12.2025).
5. Rosenberg, J. Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN) / J. Rosenberg, R. Mahy, P. Matthews, D. Wing. – Текст : электронный // IETF. – 2010. – (RFC 5766). – URL: https://datatracker.ietf.org/doc/html/rfc5766 (дата обращения: 15.12.2025).
6. Vaudenay, S. A Classical Introduction to Cryptography: Applications for Communications Security / S. Vaudenay. – New York : Springer, 2006. – 349 p. – ISBN 978-0-387-25464-7.

ПРИЛОЖЕНИЕ А

(Обязательное)

Логическая схема локальной базы данных

Вся информация пользователя, включая сообщения, контакты, ключи и служебные данные, хранится в единой локальной базе данных SQLite. Весь файл базы данных **целиком шифруется** с использованием проверенной библиотеки SQLCipher. Ключ для шифрования генерируется из мастер-пароля пользователя, что делает невозможным доступ к данным без его ведома.

На Рисунке А.1 представлена логическая структура основных таблиц базы данных.

Основные таблицы и их назначение:

- **Таблицы пользовательских данных (Peers, Chats, Messages):**
  - **Peers:** Хранит информацию об известных контактах, включая их UserID, публичные ключи RSA и уровень доверия (например, является ли контакт пиром 1-го ранга).
  - **Chats:** Содержит метаданные о существующих чатах, их участниках и свойствах (например, флаг isSecret для сокрытия чата в режиме Duress Protocol).
  - **Messages:** Основная таблица для хранения истории переписки. Каждая запись содержит полный зашифрованный "Атом сообщения", информацию об отправителе, временные метки и статус доставки.
- **Таблица кэша маршрутизации (RoutingCache):**
  - Это ключевая служебная таблица, обеспечивающая работу децентрализованной сети. В ней хранятся **временные маршруты** до других пользователей, которые не являются пирами первого ранга. Каждая запись содержит RouteID (идентификатор маршрута),

NextHopPeerID (идентификатор пира, которому нужно переслать пакет) и ExpiryTimestamp (время жизни записи, после которого маршрут считается устаревшим и требует перестроения).

- **Таблица настроек и конфигурации (Settings):**
  - Представляет собой простое хранилище типа "ключ-значение" для всех остальных служебных и пользовательских параметров. Здесь хранятся:
    - Криптографическая Salt, используемая для генерации мастер-ключей из паролей.
    - Параметры Tact Protocol (например, интервал такта).
    - Временные параметры, флаги состояния.
    - Пользовательские настройки интерфейса и поведения приложения.

Такая структура позволяет надежно и изолированно хранить как пользовательские данные, так и всю необходимую служебную информацию для обеспечения автономной работы P2P-сети.

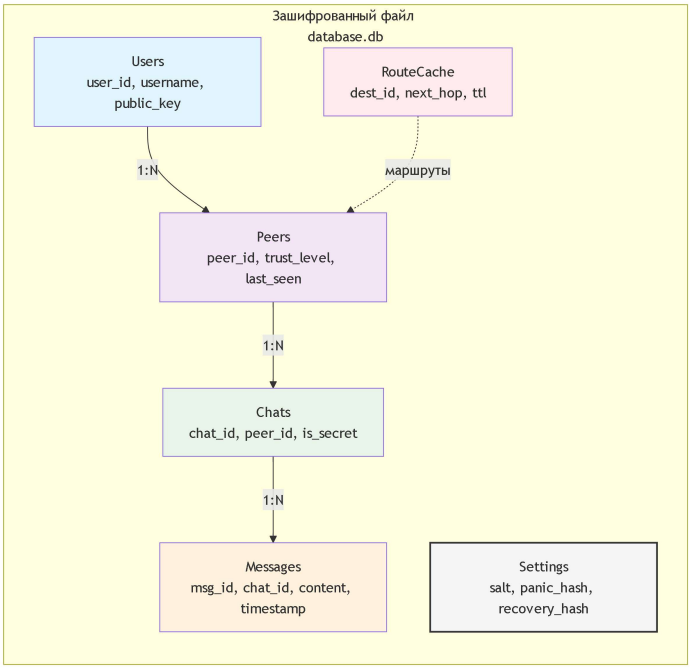

Рисунок А.1 – Логическая схема таблиц локальной базы данных D-MASH

ПРИЛОЖЕНИЕ Б

(Обязательное)

Структура кадра PhantomCall Protocol

На Рисунке Б.1 детально показана структура одного кадра данных, передаваемого по протоколу PCP. Каждый кадр является самодостаточной единицей и включает все необходимое для синхронизации, передачи полезной нагрузки и проверки целостности.

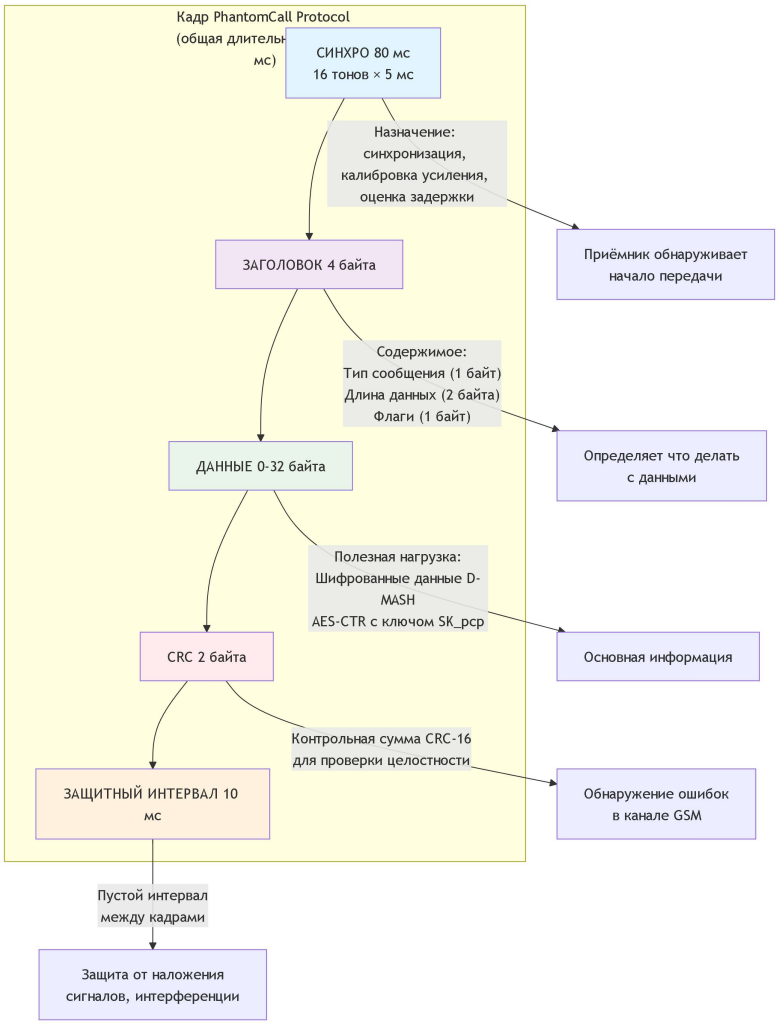

Рисунок Б.1 – Структура одного кадра данных в протоколе PCP

Описание полей кадра:

- **СИНХРО (Синхропоследовательность):** Преамбула из заранее известной последовательности тонов. Позволяет приемнику обнаружить начало кадра в аудиопотоке и откалибровать уровень сигнала.
- **ЗАГОЛОВОК:** Содержит служебную информацию о типе сообщения (сигнал тревоги, текст, координаты), длине поля данных и другие флаги.
- **ДАННЫЕ:** Полезная нагрузка — зашифрованные данные D-MASH. Поле может иметь переменную длину или отсутствовать.
- **CRC (Cyclic Redundancy Check):** Контрольная сумма, используемая для проверки целостности принятого кадра. Позволяет отбросить кадры, искаженные при передаче.
- **ЗАЩ. ИНТЕРВ. (Защитный интервал):** Короткий период тишины для разделения кадров и предотвращения межсимвольной интерференции.